US 20040139340A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0139340 A1

Johnson et al. (43) Pub. Date: Jul. 15, 2004

(54) SYSTEM AND METHOD FOR PROTECTING COMPUTER SOFTWARE FROM A WHITE BOX ATTACK

(76) Inventors: Harold J. Johnson, Ontario (CA); Stanley T. Chow, Ontario (CA); Philip A. Eisen, Ontario (CA)

Correspondence Address:
NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASINGTON, DC 20004-2128 (US)

(21) Appl. No.: 10/433,966

(22) PCT Filed: Dec. 10, 2001

(86) PCT No.: PCT/CA01/01729

(30) Foreign Application Priority Data

Dec. 8, 2000 (CA) 2 327 911

Publication Classification

(51) Int. Cl.[7] G06F 12/14

(52) U.S. Cl. 713/194; 380/1

(57) ABSTRACT

Existing encryption systems are designed to protect secret keys or other data under a "black box attack," where the attacker may examine the algorithm, and various inputs and outputs, but has no visibility into the execution of the algotitm itself. However, it has been shown that the black box model is generally unrealistic, and that attack efficiency rises dramatically if the attacker can observe even minor aspects of the algorithm's execution. The invention protects software from a "white-box attack", where the attacker has total visibility into software implementation and execution. In general, this is done by encoding the software and widely diffusing sites of information transfer and/or combination and/or loss. Other embodiments of the invention include: the introduction of lossy subcomponents, processing inputs and outputs with random cryptographic functions, and representing algorithmic steps or components as tables, which permits encoding to be represented with arbitrary nonlinear bijections.